⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平1－181349

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　平成1年(1989)7月19日
H 04 L 9/02		Z－7240－5K	
1/00		B－8732－5K	
11/00	310	Z－7928－5K	審査請求　未請求　請求項の数 4　（全7頁）

⑤4発明の名称　同報通信システム

⑳特　願　昭63－6586
㉒出　願　昭63(1988)1月14日

⑦2発明者　柳　宏　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
⑦2発明者　木原　洋一　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
⑦1出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号
⑦4代理人　弁理士　玉蟲　久五郎　外2名

明　細　書

1.発明の名称

同報通信システム

2.特許請求の範囲

(1)通信要求発生の都度暗号キーを生成し、個別接続形伝達路を経由して該暗号キーを加入者番号に対応する加入者に送達する手段と、情報を該暗号キーで暗号化し誤り訂正符号を付加し暗号化情報を形成し、これを放送形伝達路を経由して受信端末に一斉に放送的に伝達する手段とを有する情報出力装置と、

前記個別接続形伝達路を経由して受信した暗号キーと、前記放送形伝達路を経由して受信した前記暗号化情報とより元情報を復号する前記受信端末よりなることを特徴とする同報通信システム。

(2)複数の加入者番号から成る同報宛先と同報に使用する元情報を、同報要求端末から前記個別接続形伝達路を経由して前記情報出力装置に送達する手段とを備えたことを特徴とする特許請求の範囲第1項記載の同報通信システム。

(3)前記受信端末は、前記誤り訂正符号の誤り訂正が正常に行われた時に、自加入者番号と正しく受信できたことを通知する受信確認信号を前記個別接続形伝達路を経由して情報出力装置に返送する手段を備えたことを特徴とする特許請求の範囲第1項記載の同報通信システム。

(4)同報要求端末からの同報通信要求の受付ならびに前記受信端末から前記情報出力装置に返送されてきた加入者番号の一覧から成る同報通信状況の報告を、前記個別接続形伝達路を経由して同報要求端末に送達する手段を備えたことを特徴とする特許請求の範囲第1項記載の同報通信システム。

3.発明の詳細な説明

〔産業上の利用分野〕

本発明はデータ通信に関するものであつて、特に、無線伝達路あるいは多重接続機能を有する有線伝達路を用いた同報通信システムに関する。

〔従来の技術〕

第2図は従来の同報通信システムの個別接続形伝達路のブロック図である。図において、1は情報出力装置、2は個別接続形伝達路、3は受信端末である。

従来、同一の情報を複数の特定加入者に送信する同報通信システムにおいては、

(1)　有線等の個別接続形伝達路2で受信端末3と情報出力装置1を1対1に接続した後、情報の送信処理を行い、これらの動作を順次送信先の受信端末の数だけ繰り返すことにより同報通信を実現していた。

(2)　無線のような放送形伝達路を用いて同報通信を実現していた。

〔発明が解決しようとする課題〕

この(1)の方式では、以下の欠点がある。

①宛先端末ごとに逐次回線接続と送信処理が必要となるため、端末間で情報を受信する時間差が生ずる。

②時間差を少なくするためには、情報出力装置1と伝達路の途中に入る交換装置の間の回線数を増加し、さらに情報出力装置1の処理能力を向上させる必要がある。

③このため、システムが高価なものとなる。

一方、(2)の方式では、前述の問題は無くなるが、

①受信端末3を特定できない、

②通信方向が片方向であり、通信内容が受信端末側に正しく届いたか否かの確認（送達確認）が出来ない。

③第3者に通信内容が漏れてしまう。

等の問題点が発生する。

〔課題を解決するための手段〕

本発明は情報出力装置から受信端末に個別接続形伝達路と放送形伝達路との2つの伝達路を設け、個別接続形伝達路により復号化のための暗号キーの伝達ならびに送達確認の連絡を行い、放送形伝達路により同報情報の伝達を行うようにした。

〔実施例〕

(1)）第1図は本発明のシステムのブロック図、第3図は本発明の詳細なブロック図である。

1は情報出力装置、3は受信端末、4は情報、5は宛先、6は伝達確認手段、7は暗号キー生成手段、8は暗号化手段、9は誤り訂正符号付加手段、10は放送形伝達路送信手段、11は個別接続形伝達路送受信手段、12は個別接続形伝達路、13は放送形伝達路、14は同報要求端末、15は個別接続形伝達路送受信手段、20は個別接続形伝達路送受信手段、23は放送形伝達路送信手段、24は誤り訂正手段、25は暗号復号化手段を示す。

①本処理

情報出力装置1は暗号キー生成手段7で通信要求発生の都度暗号キーを生成し、個別接続形伝達路送受信手段11で個別接続形伝達路12を経由して宛先5で加入者番号（以下ＤＮ（Ｄｉｒｅｃｔｏｒｙ　Ｎｕｍｂｅｒ）と略す）に対応して指定された複数の受信端末3毎に該暗号キーを逐次送信する。

一般に、暗号キーのデータ長は、暗号化される元情報のデータ長より充分小さくできるので、暗号キーの逐次送信に要する時間及び処理負荷は極めて小さい。

一方、情報出力装置1は暗号化手段8で前記暗号キーを用いて同報要求端末より受けた同報要求の元情報を該暗号キーで暗号化し、これに誤り訂正符号付加手段9で誤り訂正符号を付加して暗号化情報を形成した後、放送形伝達路送信手段10で放送形伝達路13を経由で不特定多数の受信端末3に対し、放送により一斉に送信する。受信端末3は、この暗号化情報を受信し、誤り訂正手段24で伝送時の伝送誤りを訂正し、先に別途受信していた暗号キーを用いて暗号化情報から暗号復号化手段25により復号化する。

②同報要求処理

同報要求を行う同報要求端末14は個別接続形伝達路送受信手段15で、同報通信先である複数のＤＮから成る送信宛先と、元情報とを個別接続

形伝達路１２を経由で情報出力装置１に送信する。

③受信確認処理

受信端末３は誤り訂正が正常に行われたことを確認した時、個別接続形伝達路送受信手段２０は自ＤＮを付加した受信確認信号を個別接続形伝達路１２経由で情報出力装置１に返送する。

④同報通信状況処理

情報出力装置１はこの受信確認信号を受信し、送達確認手段６で前記受信確認信号に付加されていたＤＮと同報宛先のＤＮを比較して同報通信状況を算出する。すなわち、前記受信確認信号のＤＮから送達確認ができ、同報宛先のＤＮに含まれた前記受信確認信号のＤＮに含まれないＤＮから不達確認ができる。これにより、情報出力装置１は個別接続形伝達路送受信手段１１で前記同報通信状況を同報要求端末１４に報告し、同報要求端末１４はその同報通信状況を受信する。

以上説明したように、本発明によれば、放送形伝達路１３を用いて一斉に情報伝達が行われるために、個別接続形伝達路１２を用いた場合より安価で、受信端末３の間で情報受信時間差のない同報通信が実現できる。

放送形伝達路１３で放送される暗号化された情報は、同報宛先以外の受信端末も受信可能であるが、暗号化されているので、第３者に通信内容が漏れる心配はない。また、個別接続形伝達路１２を用いて受信確認信号を情報出力装置１に返送できるので、送達確認ができる。

この様に、受信端末３に個別接続形伝達路１２に放送形伝達路１３の２つの伝達路を組合せ、夫々の長所を生かせるシステムが構築できる。

(2) 第４図は本発明の１つの実施例のシステムブロック図で、時分割多重スイッチにより多重接続する機構（以下マルチパス機構と略す）を有する通信制御部３９対応のディジタル交換装置３１を伝達路に用いた例である。図において、３１はディジタル交換装置（マルチパス接続機構）、３２はＣＰＵ、３３は端末要求受付処理部、３４は乱数発生部、３５は暗号化処理部、３６は蓄積部、３８はＲＡＭ、３９は通信制御部、４０は誤り訂正符号処理部、４１は受信確認信号処理部、４２はＲＯＭである。ディジタル交換装置３１はＩＳＤＮ対応のマルチパス接続機構を持ち、通信制御部３９はＩＳＤＮ基本インタフエース（２Ｂ＋Ｄ）通信制御部であり、多重化された２個のＢｃｈ回線と１個のＤｃｈパケットに対する送受信制御を行う。第４図の各ブロックは情報出力装置１、同報要求端末１４、受信端末３の構成ブロックが何れも電算機と略同一構成なことを示した。第１図における個別接続形伝達路１２および放送形伝達路１３は、本実施例では、マルチパス接続機構を有するディジタル交換装置３１に縮退しており、個別接続形伝達路１２はＤｃｈパケットを用い、た伝達路に、放送形伝達路１３はＢｃｈのマルチパス接続機構を用いた伝達路に夫々対応する。まず最初に、１本のデータハイウエイに３本の端末回線が多重化されている例のマルチパス接続機構について説明する。多重度は３以上でも動作原理は同じである。

第５図はディジタル交換装置３１におけるマルチパス接続の原理の説明図である。図において、５１はタイムスロットメモリ、５２は読み出し制御メモリ、５３はクロック、５４は入データハイウエイ、５５は出データハイウエイである。タイムスロットメモリ５１によるディジタル交換動作の概要をまず説明する。複数の端末回線から入力されるディジタル信号は、タイムスロットと呼ぶ一定の長さのデータに区切られ、入データハイウエイ５４において各端末回線に１対１に対応するタイムスロットとして多重化されて運ばれる。同様に出データハイウエイ５５の上で多重化されて運ばれる各タイムスロット上の信号は、夫々対応する端末回線へ分配して送信される。Ａ、Ｂ、Ｃは、夫々端末回線＃１、端末回線＃２、端末回線＃３から入力されてデータハイウエイ上に多重化されて転送されるタイムスロット上の信号を表す。クロック５３はタイムスロットメモリ５１の書き込みをタイムスロット単位で行うタイミング及び読み出し制御メモリ５２を読み出すタイミングを供給するためのものである。タイムスロットメモ

リ５１は、入データハイウエイ５４から入力されるタイムスロットを順番にタイムスロットメモリ５１に書き込んでいく。一方、読み出し制御メモリ５２は、タイムスロットメモリ５１に書き込まれたタイムスロットを読み出す順番を記憶するためのメモリである。読み出し制御メモリ５２の内容を変更することにより、タイムスロットメモリ５１に書き込まれた順番と異なる順番でタイムスロットを読み出し、出データハイウエイ５５へ送出することが可能となり、入データハイウエイ５４と出データハイウエイ５５とでタイムスロットの順序が変わり、端末回線間の信号の交換が可能となる。

次に、以上説明したディジタル交換装置３１を使ったマルチパス接続機構を説明する。第５図において、読み出し制御メモリ５２の内容を、例えばすべて２にしておくと、出データハイウエイ５５上には全てＢが読み出され、すべての端末回線にＢが送出されることになるので、マルチパス接続機構が実現できる。端末回線＃２から入力された信号をタイムスロットメモリ５１から＃１、＃２、＃３の各端末回線に送出する時間差は、端末回線上においてタイムスロット１個を送信するのに要する時間以下である。通常のディジタル交換装置３１における交換処理の単位であるタイムスロットは、数ビットの長さしかなく、同報送信する全体の情報の長さに比してはるかに小さいので、本マルチパス接続機構による同報時間差は事実上無視でき、放送形伝達路と同等の機能を持つものと考えられる。

次に本実施例の動作を説明する。

①本処理

第６図は実施例の動作概要の流れ図である。同報送信に先立ち、種々の同報通信要求で選択される可能性のある全ての受信端末３と情報出力装置１をマルチパス接続できるように、ディジタル交換装置３１の読み出し制御メモリ５２の内容は、前述した方法で事前に設定しておく。すなわち、前記マルチパス接続機構により、受信端末３のＢｃｈ回線が空きの状態のときには、該Ｂｃｈ回線を情報出力装置１のＢｃｈ回線に接続されるようにしておくようにする。これにより、情報出力装置１およびディジタル交換装置３１は、情報出力装置１とＤＮで指定される受信端末３との間の接続処理を同報呼の生起する毎に行わずに、情報出力装置１からの送信情報を、時間差なく、マルチパス接続された全ての受信端末３に送出することが可能となる。従つて、従来の同報通信システムが１対１の接続を逐次あるいは複数回線を使っていたのに比較して、接続および情報送信の処理負荷が格段に低減し、また、情報出力装置１側の回線が１回線のみですむので、はるかに経済的なシステムとなる。この効果は、同報の宛先数が多くなるほど顕著である。

この様な状況で同報通信要求が発生すると、まず、情報出力装置１は乱数を発生し、暗号キーとする。この暗号キーを同報宛先５で指定される受信端末３に対し、Ｄｃｈパケットで順次送信していく。受信端末３は暗号キーを受信するとともに、Ｂｃｈを他の端末が使用しないように閉塞する。

情報出力装置１は、前記暗号キーで送信の元情報を暗号化し、誤り訂正符号を付加して暗号化情報を形成し、Ｂｃｈ経由でディジタル交換装置３１に送出する。ディジタル交換装置はマルチパス接続機構で、同報宛先に無関係に不特定の受信端末に対し情報出力装置１から受けた情報をＢｃｈを用いて送出する。受信端末３はＢｃｈで受信した暗号化情報の誤り訂正を行い、前記方法で受信した暗号キーで復号する。

②同報要求処理

まず同報要求端末１４は同報送信を依頼する情報と同報宛先をＤｃｈパケットを用いて情報出力装置１に送出する。情報出力装置１は同報要求端末１４からの送信情報と同報宛先を受信する。以後の動作は前述のとおりである。

③受信確認処理

受信端末３は誤り訂正が正しく行われた時点で、Ｄｃｈパケットを用いて情報出力装置１に受信確認信号を返送する。Ｄｃｈパケットは発信者識別番号が自動的に付加されるため、受信確認信号に

は受信端末3のDNが付加されている。また、受信端末3が受信確認信号返送時に使用する情報出力装置1のDNは、暗号キー受信時入力Dchパケットに付加されてくる発信者識別番号を用いればよい。情報出力装置1は受信確認信号を受信し、受信確認信号に付加されているDNから正しく通信できた受信端末3を知り、同報宛先と比較することで正しく通信できなかつた受信端末3を知ることができる。

④同報通信状況処理

情報出力装置1は正しく通信できた受信端末3のDN及び正しく通信できなかつた受信端末3のDNの一覧から成る同報通信状況を、Dchパケットを用いて同報要求端末14に送出する。

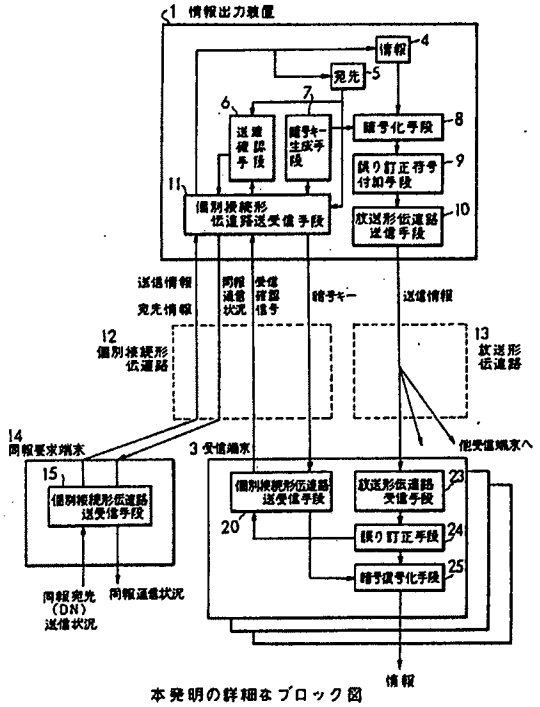
〔発明の効果〕

本発明によれば、個別接続形伝達路と放送形伝達路を組合せることで、第3者に通信内容が漏れることのない、送達確認が可能な、端末間で受信時間差のない経済的な同報通信システムを提供することができる。

4.図面の簡単な説明

第1図は本発明のシステムのブロック図、第2図は従来の同報通信システムの個別接続形伝達路のブロック図、第3図は本発明の詳細なブロック図、第4図は本発明の1つの実施例のシステムブロック図、第5図はデイジタル交換装置のマルチパス接続の原理の説明図、第6図は実施例の動作概要の流れ図である。

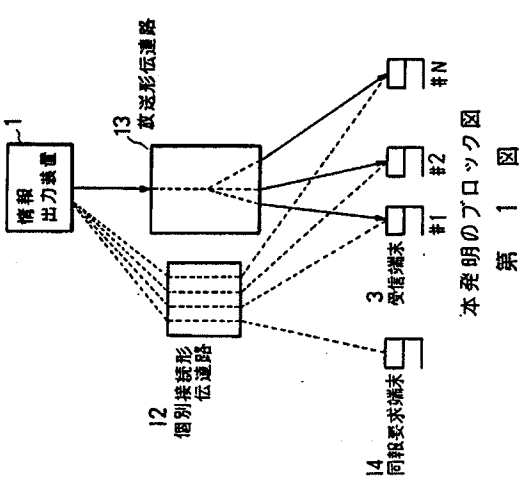
1は情報出力装置、2は個別接続形伝送路、3は受信端末、4は情報、5は宛先、6は送達確認手段、7は暗号キー生成手段、8は暗号化手段、9は誤り訂正符号付加手段、10は放送形伝達路送信手段、11は個別接続形伝達路送受信手段、12は個別接続形伝達路、13は放送形伝達路、14は同報要求端末、15は個別接続形伝達路送受信手段、20は個別接続形伝達路送受信手段、23は放送形伝達路受信手段、24は誤り訂正手段、25は暗号復号化手段、31はデイジタル交換装置、32はCPU、33は端末要求受付処理部、34は乱数発生部、34は暗号化処理部、36は蓄積部、38はRAM、39は通信制御部、40は誤り訂正符号処理部、41は受信確認信号処理部、42はROM、51はタイムスロツトメモリ、52は読み出し制御メモリ、53はクロツク、54は入データハイウエイ、55は出データハイウエイ、DNは加入者番号。



本発明の詳細なブロック図

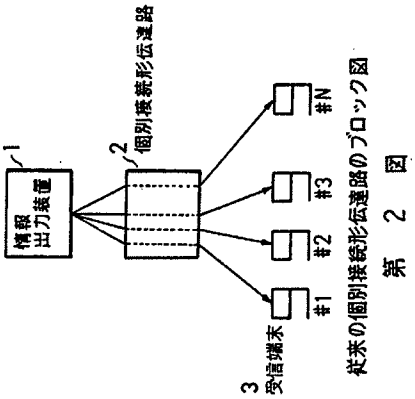
第　3　図

特許出願人　日本電信電話株式会社
代理人　弁理士　玉　蟲　久五郎
（外2名）



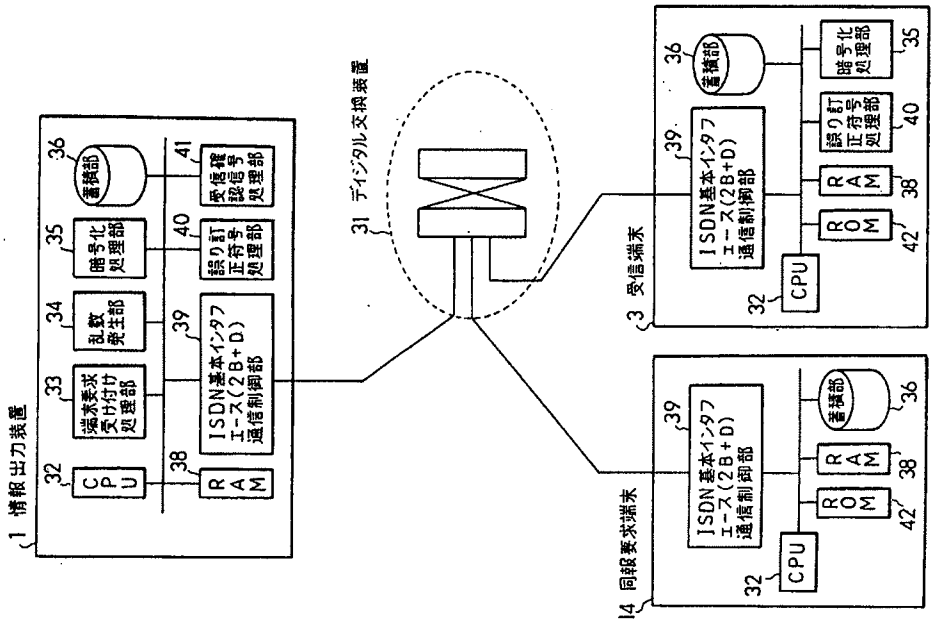
本発明のブロック図

第　1　図



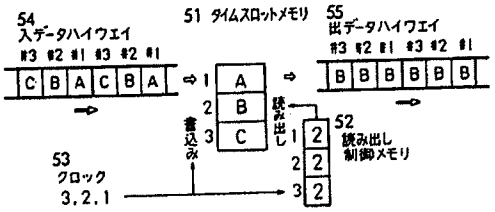
従来の個別接続形伝達路のブロック図

第　2　図



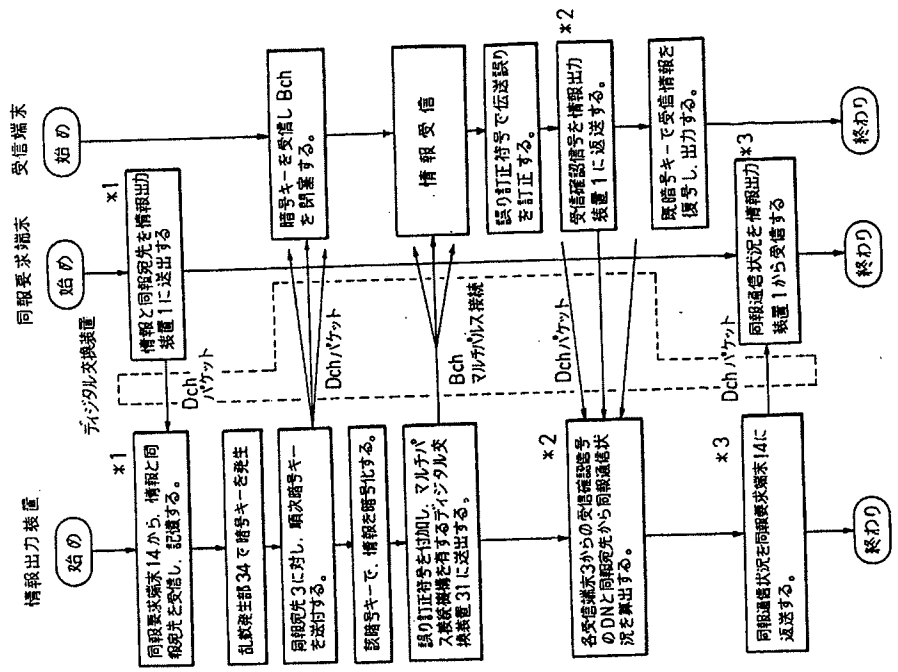
実施例のシステムブロック図

第　4　図



マルチパス接続の原理の説明図

第　5　図



注）＊1：特許請求範囲第3項及び第4項において追加される動作
＊2：特許請求範囲第2項において追加される動作
＊3：特許請求範囲第4項において追加される動作

実施例の動作概要の流れ図

第　6　図

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **01-181349**

(43)Date of publication of application : **19.07.1989**

(51)Int.Cl. **H04L 9/02**
H04L 1/00
H04L 11/00

(21)Application number : **63-006586**

(22)Date of filing : **14.01.1988**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

(72)Inventor : **YANAGI HIROSHI**
KIHARA YOICHI

(54) MULTIPLE ADDRESS COMMUNICATION SYSTEM

(57)Abstract:

PURPOSE: To obtain an economical multiple address communication system where the content of communication is not leaked to a 3rd party and there is no reception time difference between terminal equipments enabling the confirmation of transmission by combining an individual connection type transmission line and a broadcast type transmission line.

CONSTITUTION: Two transmission lines of individual connection type transmission line 12 and broadcast type transmission line 13 are provided from an information output device 1 to a reception terminal equipment 3. Then the transmission of a cryptographic key for decoding and the communication of transmittal confirmation are applied through the individual connection type transmission line 12 and the multiple address information is sent through the broadcast type transmission line 13. Thusthere is no care about the leakage of the content of communication to the 3rd party and the transmission is confirmed and the inexpensive multiple address communication system is obtainedwhere there is no reception time difference between terminal equipments.